What is claimed is :

1. A compression method of digital signature, wherein

a sender,

generates a digest by compressing data to be sent by a predetermined compression procedure, creates a cryptographic digest by enciphering the digest with a secret key of the sender, and at the same time, sends the cryptographic digest by attaching to the data as a signature text, and

a receiver,

restores an original digest by decoding the received cryptographic digest with a public key of the sender, and at the same time, generates a digest of a reception data by compressing the received data with said compression procedure, and validates the legitimacy of the data by comparing the digest of said reception data with the restored original digest, wherein

said compression procedure comprises the steps of:

inputting series of numerals of an arbitrary length and arranging in a matrix of n x n by a predetermined arrangement procedure,

outputting as a compressed numeral the series of numerals of n + n columns in length and width composed of algebraic values taken as modulo 10 which is an addition value of respective digits in the line direction and row direction of said matrix of n x n, and

reiterating said steps up to the end of input of the series of numerals.

2. The compression method of digital signature of claim 1, wherein said arrangement procedure comprises the steps of:

arranging series of numerals along diagonals of said matrix, and

arranging the remaining series of numerals in a frame other than the diagonals of the matrix.

3. The compression method of digital signature of claim 1, wherein said arrangement procedure comprises the steps of:

generating and delivering an arrangement key by the sender and the receiver, and arranging series of numerals according to an arrangement order specified by said arrangement key.

4. The compression method of digital signature of claim 1, wherein,

when said series of numerals are input to arrange into a matrix,

they are arranged by mixing with the series of numerals input the compressed numerals of n + n columns in length and width output in the previous step.